

WHAT IS CLAIMED IS:

1. A monitor system comprising:
a packet reader configured to scan packets transmitted through a network for pre-specified criteria, wherein the packets include endpoint information and data;
a request/response matcher configured to receive packets that meet the pre-specified criteria from the packet reader, and to match request packets with corresponding response packets; and
a message analyzer configured to access the matched packets, determine the structure utilized in the data of the matched packets, and to analyze the data of the matched packets to generate at least a portion of a model of the data.
2. The monitor system according to Claim 1 wherein the request/response matcher and the message analyzer are configured to access a database to store and retrieve the matched packets.
3. The monitor system according to Claim 1 wherein the packet reader is configured to decipher and reformat the header and data in the packets.
4. The monitor system according to Claim 1 further comprising:
computer executable instructions configured to monitor transactions between components in the network based on the matched packets.
5. The monitor system according to Claim 1 further comprising:
computer executable instructions configured to provide information regarding the matched packets to an application program in the network.
6. The monitor system according to Claim 1 further comprising:
computer executable instructions configured to provide information regarding the matched packets to a network administration facility for the network.

7. The monitor system according to Claim 1 further comprising:
computer executable instructions configured to validate the data in subsequent
packets based on the data model.
8. The monitor system according to Claim 1 further comprising:
computer executable instructions configured to log statistical information
regarding the matched packets.
9. A monitor system comprising:
computer executable instructions configured to generate a map of the packets
transmitted between endpoints in a network.
10. The monitor system according to Claim 9 further comprising:
computer executable instructions configured to determine the type of application
in which the matched packets are utilized.
11. The monitor system according to Claim 1 wherein the monitor system is
implemented within a server in the network.
12. The monitor system according to Claim 1 wherein the monitor system is
configured to monitor the packets for a plurality of servers in the network.
13. The monitor system according to Claim 1 further comprising:
computer executable instructions configured to combine the data from a plurality of
related packages to form a message.
14. A method for monitoring network traffic comprising:
intercepting packets prior to delivering the packets to their destination;
determining whether the packets match a pre-defined format; and
matching request and response packets among the packets that match the pre-
defined format.

15. The method according to Claim 14, wherein the packets include headers with endpoint information, and data, the method further comprising:
combining the data from a plurality of related packages to form a message.
16. The method according to Claim 15, further comprising:
determining the content of the message.
17. The method according to Claim 14, wherein the packets include headers with endpoint information and data, further comprising:
determining traffic flow of the packets in the network based on the endpoint information.
18. The method according to Claim 1, further comprising:
generating at least a portion of a data model based on information in related packets.
19. The method according to Claim 18, wherein the packets include headers with endpoint information and data, further comprising:
generating a map of the packets transmitted between the endpoints in the network;
and
providing the data model to other components to enable the other components to communicate with the endpoints. .
20. The method according to Claim 15, further comprising:
logging statistical information regarding the matched packets.
21. The method according to Claim 18, further comprising:
analyzing the data model for information regarding the security of the message;
and
preventing messages that include confidential information from being transmitted to their destination.

22. The method according to Claim 19, further comprising:
preventing unvalidated messages from being transmitted to their destination.
23. An apparatus comprising:
means for intercepting packets prior to delivering the packets to their destination,
wherein the packets include headers with endpoint information, and data;
means for determining whether the packets match a pre-defined criteria; and
means for generating at least a portion of a data model for the data in the packets
that match the pre-defined criteria.
24. The apparatus according to Claim 23, further comprising:
means for matching request and response packets among the packets that match
the pre-defined criteria; and
means for mapping traffic flow between components in a network based on the
endpoint information and the data model.
25. The apparatus according to Claim 23, further comprising:
means for combining the data from a plurality of related packages that meet the
pre-defined criteria to form a message;
means for validating the message based on the data model; and
means for preventing unvalidated messages from being transmitted to their
destination.
26. The apparatus according to Claim 23, further comprising:
means for generating a table of the data model and endpoints that transmit packets
that conform to the schema
27. The apparatus according to Claim 25, further comprising:
means for analyzing the data model for information regarding the security of the
message; and
means for preventing messages that include confidential information from being
transmitted to their destination.